Advisory Alert

Alert Number: AAA20260612 **Date:** June 12, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
Oracle	**Critical**	Remote Code Execution Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Hitachi	**High**	Security Update
MongoDB	**High**	Use-After-Free Vulnerability
Check Point	**Medium**	Local Privilege Escalation Vulnerability

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31419, CVE-2026-31467, CVE-2026-31532, CVE-2026-31581, CVE-2026-43037, CVE-2026-43501, CVE-2026-46054)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 10 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.2 x86_64 Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.2 s390x Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.2 ppc64le Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.2 aarch64 Red Hat CodeReady Linux Builder for x86_64 10 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le Red Hat CodeReady Linux Builder for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.2 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.2 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.2 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.2 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.2 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 10.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 10.2 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 10.2 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 10.2 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:25191

Vendor	**Oracle**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-35273)
Description	Oracle has released a security update addressing a vulnerability that exists in their products. **CVE-2026-35273:** Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Updates Environment Management). Supported versions that are affected are 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PeopleSoft Enterprise PeopleTools versions 8.61, 8.62
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/alert-cve-2026-35273.html

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23216, CVE-2026-31419, CVE-2026-31508, CVE-2026-31581, CVE-2026-43037, CVE-2026-43056, CVE-2026-43116, CVE-2026-43125, CVE-2026-43501, CVE-2026-45852, CVE-2026-46181, CVE-2025-40170, CVE-2025-40135, CVE-2025-40158, CVE-2025-68724, CVE-2025-71089, CVE-2025-71116, CVE-2026-22984, CVE-2026-22990, CVE-2026-23455, CVE-2026-43110, CVE-2026-43190)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:25217 • https://access.redhat.com/errata/RHSA-2026:25218

Vendor	**Hitachi**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2025-7737)
Description	Hitachi has released a security update addressing a vulnerability that exists in their products. **CVE-2025-7737:** When a large number of malicious packets are received, the iSCSI port may become unresponsive. Hitachi advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Hitachi Virtual Storage Platform 5100, 5500, 5100H, 5500H • Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H • Hitachi Virtual Storage Platform E390, E590, E790, E990, E1090, E390H, E590H, E790H, E1090H • Hitachi Virtual Storage Platform G130, G150, G350, G370, G700, G900 • Hitachi Virtual Storage Platform G100, G200, G400, G600, G800 • Hitachi Virtual Storage Platform F400, F600, F800 • Hitachi Virtual Storage Platform G1000, G1500 • Hitachi Virtual Storage Platform F1500 • Hitachi Virtual Storage Platform VX7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/2026_312.html

Vendor	**MongoDB**
Severity	**High**
Affected Vulnerability	Use-After-Free Vulnerability (CVE-2026-11933)
Description	MongoDB has released a security update addressing a vulnerability that exists in their products. **CVE-2026-11933:** A use-after-free vulnerability exists in MongoDB Server's server-side JavaScript engine when converting BSON documents to JavaScript arrays. An authenticated user with read privileges who is able to run server-side JavaScript (for example, via $where or $function) can cause the server to access memory that has already been freed. This may result in disclosure of information from the mongod process memory or a denial of service through a server crash. MongoDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MongoDB: • 8.3.0 affects 8.3.3 and prior versions • 8.2.0 affects 8.2.10 and prior versions • 8.0.0 affects 8.0.25 and prior versions • 7.0.0 affects 7.0.36 and prior versions • 6.0 affects 6.0.28 and prior versions • 5.0 affects 5.0.33 and prior versions • 4.4.0 affects 4.4.30 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://jira.mongodb.org/browse/SERVER-128125

Vendor	**Check Point**
Severity	**Medium**
Affected Vulnerability	Local Privilege Escalation Vulnerability (CVE-2026-10847)
Description	Check Point has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-10847:** A vulnerability in the Identity Agent log collection mechanism could allow an authenticated local user to execute code with elevated privileges on the Windows endpoint computer under specific conditions. Check Point advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Identity Agent Full - for Windows OS version 81.087.0000
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk185052

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.